09/187,700 Proposed Claim Amendments

1. (Marked up) A storage medium data protecting method of protecting data on a storage medium having a plurality of unit areas, comprising:

a step of generating a random key [[data]], encrypting [[the]] said random key [[data]] with a password, and writing [[the]] said encrypted random key [[data]] to [[said]] the storage medium;

a step of encrypting the data with [[the]] said generated random key [[data]], and writing [[the]] said encrypted data to [[said]] the storage medium;

a step of reading [[the]] said encrypted key data from [[said]] the storage medium;

a step of decoding [[the]] said encrypted key data with [[the]] said password; and

a step of decoding the data on [[said]] the storage medium with [[the]] said decoded key data,

wherein said random key [[data]] generating step comprises:

a step of generating a different random key [[data]] for each [[of a plurality of]] unit storage area of the plurality of unit storage areas [[of said storage medium]], so that said each unit storage area is assigned a different random key than any other of the plurality of unit storage areas, and said assignment of said different random key to said each unit storage area being based on a particular unit storage area to which the data, once encrypted, is to be stored;

a step of encrypting each of said different random [[key data for each unit storage area]] keys with said password, and

a step of writing each of said encrypted key data to [[said]] the storage medium,

wherein said data encrypting step comprises a step of encrypting the data with [[the]] said random key [[data]] corresponding to its said particular unit storage area to write the data, and

wherein said data decoding step comprises a step of decoding the data with [[the]] said decoded key data corresponding to said particular unit storage area where the data have been read.

PAGE 3/5 * RCVD AT 3/10/2004 4:07:52 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/1 * DNIS:7465451 * CSID:312 360 9315 * DURATION (mm-ss):01-10

1. (Clean form) A storage medium data protecting method of protecting data on a storage medium having a plurality of unit areas, comprising:

a step of generating a random key, encrypting said random key with a password, and writing said encrypted random key to the storage medium;

a step of encrypting the data with said generated random key, and writing said encrypted data to the storage medium;

a step of reading said encrypted key data from the storage medium;

a step of decoding said encrypted key data with said password; and

a step of decoding the data on the storage medium with said decoded key data,

wherein said random key generating step comprises:

a step of generating a different random key for each unit storage area of the plurality of unit storage areas, so that said each unit storage area is assigned a different random key than any other of the plurality of unit storage areas, and said assignment of said different random key to said each unit storage area being based on a particular unit storage area to which the data, once encrypted, is to be stored;

a step of encrypting each of said different random keys with said password, and

a step of writing each of said encrypted key data to the storage medium,

PAGE 4/5 * RCVD AT 3/10/2004 4:07:52 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/1 * DNIS:7465451 * CSID:312 360 9315 * DURATION (mm-ss):01-10

wherein said data encrypting step comprises a step of encrypting the data with said random key corresponding to its said particular unit storage area to write the data, and

wherein said data decoding step comprises a step of decoding the data with said decoded key data corresponding to said particular unit storage area where the data have been read.

PAGE 5/5 * RCVD AT 3/10/2004 4:07:52 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/1 * DNIS:7465451 * CSID:312 360 9315 * DURATION (mm-ss):01-10 TAI P 05